REMARKS

Claims 1-41 are currently pending in the subject application, and are presently under consideration. Claims 1-41 are rejected. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 1-41 Under 35 U.S.C. §103(a)

Claims 1-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Funk (U.S. 5,721,779) in view of Keene, et al. (U.S. PG Pub. No. 2004/0049294). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 1 recites a method of administering access and security on a network having a plurality of computers. Messages broadcast or multicast within the network are filtered and displayed as-permitted by the associated privileges when a user's password is matched with the one-way encrypted password file. Claim 20 recites a system to administer access and security on a network having a plurality of computers. The system includes a channel monitoring and filtering module to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message. Finally, claim 31 recites a computer program for administering access and security on a network having a plurality of computers. The program includes a channel monitoring and filtering code segment to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message.

It is respectfully submitted that Funk in view of Keene do not teach or suggest the filtering and display of broadcast or multicast messages based upon user privileges associated with a one-way encrypted password as recited in claims 1, 20, and 31, either alone or in combination. The Office Action states that Keene provides a teaching of broadcasting and/or multicasting a message based on the ability of an authenticated user with modification privileges in Keene to alter an object on a central server. The Office Action asserts that the altered message is a broadcast message as it provides a form of data exchange between the modifying user and

other authenticated users on the network. It is respectfully submitted that this form of exchange does not comprise a broadcast or multicast message.

Webster's dictionary defines the term broadcast as "cast or scattered in all directions." A computer specific definition, provided by Symantec Security, is "sent simultaneously to all users on a network." These definitions are consistent with the meaning of the claim; in the present invention, a broadcast message is sent out simultaneously in all directions or to all users. The broadcast message is not sent solely to authenticated users, but broadcast over the airwaves or sent to all or a plurality of users on a network. A plurality of users, authenticated and unauthenticated, receives every message broadcast across the network, but the messages are filtered at each of the plurality of computers to restrict the access according to the user's associated privileges. This differs from the characterization of the Keene patent in the Office Action, as the "message" is a modification of an object at the central server. No message is sent simultaneously to all users (*i.e.*, broadcast) or even to a plurality of intended recipients (*i.e.*, multicast) in Keene. There is no teaching of the distributed filtering of the present invention. To the extent that a message is provided to any users, it is accessed individually by each authenticated user upon a request to the server, it is not broadcast or multicast to a plurality of users. It is thus respectfully submitted that the rejection of claims 1, 20, and 31 should be withdrawn.

Turning to the dependent claims, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claims 5, 26, and 37 recite spoofing the user into believing that the access has been gained to the computer upon request of the systems administrator or security officer, wherein spoofing includes the presentation of false messages and information to the user.

Neither of the cited references discuss spoofing an unauthenticated user into believing that access has been gained in the computer system. The Office Action states that the generation

of random signals and authentication values in Funk comprises providing false data to the user. It is respectfully submitted that nothing in Funk teaches or suggests providing false data to a user for the purpose of deceiving the user into believing that access to the computer has been achieved. The claims recite spoofing the user into believing that access has been gained in the computer system, not simply providing false data. Keene also fails to teach or suggest spoofing a user who is accessing the system. Accordingly, it is respectfully submitted that claims 5, 26, and 37 are nonobvious and patentable over the cited art.

Claims 6, 25, and 36 recite disabling a computer system to prevent access by the user upon a request by the system administrator. Neither cited reference contains a teaching of disabling the system upon one or more rejections of user provided authentication. As discussed above, Funk and Keene simply provided for the rejection incorrect passwords and do not teach or suggest further action in response to multiple failed log-on attempts. The cited passage in Funk simply describes a randomization process for the encryption keys used in the authentication process. There is no discussion in the cited passage of disabling a user's computer in response to a request by a system administrator. At best, Funk and Keene teach denying access to a central server upon a request from a system administrator. The Office Action does not clarify the relevance of the cited passage, despite the arguments in the prior amendment. Accordingly, it is respectfully submitted that claims 6, 25, and 36 are nonobvious and patentable over the cited art.

Claim 7 recites deleting a plurality of files from a user's computer system upon a request by the systems administrator or security officer. Claims 25 and 36, discussed above, also include this element. Neither reference discusses remotely deleting system files to prevent an unauthorized user from accessing them. The Office Action cites a passage within Funk, discussing the encrypted challenge and response process used in authenticating in a user. There is no discussion in the cited passage of deleting files from a user's computer in response to a request by a system administrator. Again, Funk and Keene merely teach denying access to a central server upon a request from a system administrator. The Office Action does not clarify the relevance of the cited passage, despite the arguments in the prior amendment. It is thus respectfully submitted that claims 7, 25, and 36 are nonobvious and patentable over the cited art.

Claims 8, 28, and 39 recite displaying a request for reauthentication at the direction of a system administrator or security officer. Claim 9, which depends from claim 8, requires that this reauthentication will take the form of a displayed log-in screen having a position for entry of the user identification and password. The Office Action cites two passages in Funk describing an initial authentication procedure. The claims, however, discuss reauthentication, requiring an already authenticated user to reenter a user identification and password just to maintain the present connection upon the request of a system administrator. Neither of the cited references discusses such a reauthentication process. The Office Action does not clarify the relevance of the cited passage, despite the arguments in the prior amendment. It is thus respectfully submitted that claims 8, 28, 39, and 9 are nonobvious and patentable over the cited references.

Claim 11, which depends from claim 9, recites a method further including the following steps. A master password file is accessed on a computer system accessible to the system administrator or security officer. The password is one-way encrypted, and the master password file is searched for a match of the user identification and the one-way encrypted password. Claim 13, which depends from claim 11, adds the following steps. An authenticated user enters a new password. The user identification and password stored on the master password file is reauthenticated. The new password is one-way encrypted, and the user identification and password in the master password file are replaced with the new user identification and the new one-way encrypted file.

Neither Funk nor Keene teach or suggest a password updating process initiated by a reauthentication request by the system administrator or security officer. The Office Action cites a passage within the Funk, discussing the encrypted challenge and response process used in authenticating in a user, but does not provide the required teaching. The Office Action does not clarify the relevance of the cited passage, despite the arguments in the prior amendment. Accordingly, claims 11 and 13 are patentable over the cited art.

Claims 14, 29, and 40 recite attaching a master password file to a message, encrypting the message with a private key and passphrase available only to the systems administrator or security officer, and transmitting the message to the plurality of computers. Neither of the cited

references contains such a teaching. The Office Action cites a passage in Funk discussing its challenge protocol in rejecting this claim. The cited passage does not address reauthorization or the updating of passwords on individual computers in the network. The Office Action does not clarify the relevance of the cited passage, despite the arguments in the prior amendment. Keene does not remedy this deficiency. Accordingly, it is respectfully submitted that claims 14, 29, and 40 are thus nonobvious and patentable over the cited art.

Claims 15, 30, and 41 recite decrypting a message using a public key corresponding to the private key, reporting to the system administrator any failure to decrypt the message and replacing the one-way encrypted password file with the decrypted master file. The claims further recite notifying a system administrator if it receives a master password file that it cannot encrypt. This is intended to notify the system administrator of any attempts by an intruder to impersonate the system administrator. When the public key for the administrator fails to match the encryption key used for the file, it can be assumed that the file has been tampered with or otherwise falsified. Neither of the cited references teaches or suggests such a verification method. The passage cited in the Office Action discusses a method for updating passwords, but does not teach notifying the system operator. The Office Action does not clarify the relevance of the cited passage, despite the arguments in the prior amendment. It is thus respectfully submitted that claims 15, 30, and 41 are nonobvious and allowable over the cited art.

Dependent claims 2-19, 21-30 and 32-41 depend directly or indirectly from independent claims 1, 20, and 31, respectively. The applicant asserts that these claims are nonobvious and patentable for the reasons discussed above under their respective base claims and for their own unique elements.

For the reasons described above, claims 1-41 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 12/21/04

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072